mesa·az

City Auditor

Date: September 17, 2008

To: Audit and Finance Committee

From: Gary Ray, City Auditor

Subject: Credit Card Security Review

Pursuant to the Council-approved audit plan the City Auditor's Office has completed its review of the City's compliance with the Payment Card Industry's Data Security Standards (PCI DSS). Our review focused on day-to-day processing activities, with the purpose of assisting in the City's PCI DSS compliance efforts.

An overview of our recommendations for ensuring compliance is below. In following with the PCI DSS requirement to annually assess compliance, we will follow-up on the departments' implementation of our recommendations and begin new reviews on all of the City's credit card processing sites in about one year.

We would like to thank each department's management and staff for their cooperation, professionalism, and assistance throughout the review process.

If you have any questions please feel free to contact me at x3210 or Jason Taylor at x3635.

Background

The PCI Security Standards Council was founded by the major payment card brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc) to develop and manage a uniform set of security standards. They developed the PCI DSS in January 2005, and updated them to the current version in September 2006. The general requirements of the PCI DSS are as follows:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

All merchants are required to comply with PCI DSS, as regulated by their acquiring banks. Failure to do so could result in fines of up to $500,000 per compromise.

Summary of Recommendations

Our general recommendations to ensure compliance are explained below. These have been communicated to the appropriate staff. Most departments have begun implementing the recommendations, with several departments indicating that they have already fully implemented them.

1. **Ensure that background checks are performed**
   The City did not have a record of background checks for 2 of 25 employees sampled with credit card handling responsibilities. To reduce the risk of internal fraud, the City's Human Resources department should identify whether any other credit card processors are missing background checks, and perform them as necessary.

2. **Implement controls over sensitive credit card information**
   Departments need to better protect sensitive credit card information, such as receipts and forms displaying full credit card numbers. Failure to protect this information can allow unauthorized users to obtain and use it for fraudulent purposes. We recommend the following:

   - **Physically secure and restrict access to sensitive information**—This includes locking the information in such places as drawers, cabinets, or safes, and limiting access to those employees whose job duties require it. Further, until the City's offsite storage vendor, Recall, achieves PCI DSS compliance certification, departments that store information with the vendor should place the information in document lock boxes, to better restrict access.

   - **Implement access logging and inventory procedures**—Departments that have physically secured their sensitive credit card information, either onsite or with Recall, should implement controls such as access logs and inventories that are reviewed by independent employees. Without such controls, stolen or missing information could go unnoticed indefinitely. Departments with smaller data stores may instead choose to manually redact the credit card numbers on the information, such that only the last 4 digits of the card numbers are readable.

- **Refrain from improper storage**—One of the tenets of PCI DSS is that sensitive information should not be stored if it is not needed. To minimize sensitive credit card information that needs to be secured, the Accounting Services Division should continue transitioning departments' PIN PAD devices to those that do not display credit card numbers on merchant copy receipts.

  In addition, PCI DSS explicitly prohibits the storage of credit card security/validation codes, as they make it easy for individuals to execute fraudulent Internet and mail order/telephone order transactions.

- **Improve destruction procedures for credit card information**—Departments must periodically destroy credit card information that is beyond its retention period or inappropriate to store. However, if sensitive credit card information is ineffectively disposed of, the information could be recovered and used for fraudulent purposes. When destroying information themselves, departments should use crosscut shredders. When authorizing one of the City's document destruction vendors do destroy documents, departments should obtain certificates of destruction.

3. **Secure processing systems**
   All departments should safeguard their credit card processing systems by using unique passwords. Failure to do so could allow unauthorized individuals to access city applications and sensitive information – credit card or otherwise – which could result in fraudulent use. The number of employees whose job duties involve those functions should be limited, and only they should know the passwords. The passwords should be actively managed such that they are not the default passwords, and they are changed periodically, including when there is staff turnover and when the passwords are thought to have been compromised. Departments should physically secure processing systems that cannot be password protected or are inconsistently used, such as older PIN PAD devices.

4. **Follow data retention schedules**
   Departments should destroy all credit card information that is beyond the 3 year retention period – being sure to obtain certificates of destruction from Recall, as appropriate – and continue to follow the 3 year retention schedule. Extended storage of cardholder data that exceeds business need creates an unnecessary risk that the data could be stolen and used for fraudulent purposes. Conversely, destroying documents too early results in non-compliance with the State's record retention requirements. It could also limit the City's ability to effectively resolve disputes, which would in turn result in chargebacks to the City.

5. **Develop department-specific procedures**
   PCI DSS require merchants to develop credit card security procedures to serve as "desk instructions" for employees. Failure to do so could result in employees not properly securing all sensitive information or resources, which could in turn lead to a breach. Accounting Services has communicated various security procedures in its Credit Card Handling class. However, each department should develop specific procedures that address its unique business environment. In addition, departments should require employees to acknowledge in writing that they have read and understood the Citywide and department-specific security policies and procedures.